ADMINISTRACIÓN DE UNIX

Introducción

La administración es el mantenimiento rutinario necesario para que un sistema crezca y se modifique. Las siguientes son tareas que caen en la categoria del sistema:

El ingreso y la retirada de los ids de presentacion de usuario
La instalacion de nuevo software
La eliminacion de ficheros de registro
El formateo de discos flexibles
Realizacion de copias de seguridad

La administracion del sistema es vital, incluso en una maquina Unix de un solo usuario. Aunque las tareas de administracion son significativamente mas complejas sobre un sistema multiusuario sobre un sistema MS-DOS, las versiones mas recientes del sistema Unix han producido herramientas mejoradas que pueden facilitar estas tareas. En particular el Unix del Open Desktop provee el programa Sysadmsh (System Administration Shell), que hace que la administracion sea mucho mas facil de lo que nunca antes habia sido. El Sysadmsh incluye menus de pantalla completa y formilarios para entrada de dato con buenas facilidades de verificacion de errores. Incluso los expertos tienden a utilizar esta herramienta en vez de los metodos manuales.

Sin embargo, la mayoria de los agentes de usuarios como el Sysadmsh estan diseñados para usuarios que entienden la idea que hay detras de los procedimientos manuales. Aunque los agentes de usuario puedan facilitar una tarea que contiene varios pasos y proporcionan listas de operaciones y alguna comprobacion de error para cada paso, no eliminan la necesidad de entender los conceptos subyacentes.

Encendido y Apagado

Generalmente hay varios procesos ejecutandose en una maquina Unix al mismo tiempo. Consiguientemente es muy peligroso desconectar la maquina cuando se ha terminado de utilizar. El sistema Unix dispone de herramientas expresamente diseñadas para crear una secuencia ordenada de sucesos cuando se desconecta la maquina. Esta secuencia es conocida como el proceso de desconeccion (shutdown), y deberia de ser seguida cuidadosamente para asegurar la sanidad del sistema cuando se arranque la maquina de nuevo. El procedimiento de arranque es complejo y existen herramientas para arrancar (boot) la maquina correctamente cuando sea enchufada. Aqui se realizaran los pasos que el sistema sigue durante los pasos de conexion y desconexion, tambien se mencionara brevemente algunos de los estados (init) que puede adoptar el sistema, ademas de que se mencionaran algunos de los problemas comunes que pueden darse en los procedimientos de arranque.

El entorno del sistema en curso.

Cuando el sistema Unix esta funcionando correctamente, es probable que haya muchos procesos activos. Naturalmente los demonios del sistema siempre estaran ejecutandose y el administrados del sistema conectado a la consola dispondra de un Shell y posiblemente algunos otros programas asociados con la sesion. Ademas, otros usuarios pueden estar presentes en la maquina desde terminales remotas, estos usuarios pueden estar ejecutando programas. Ademas las transferencias de datos subordinadas por correo electronico o uucp pueden estar corriendo en cualquier momento, y la impresion de trabajo puede estar en progreso. Finalmente, la falta de sincronizacion de los buffers en memoria y en el disco rigido del sistema significa que los contenidos reales del disco y sus contenidos logicos diferiran. Es decir, cuando se escribe un fichero desde el editor, el fichero no estara actualizando en disco hasta segundos o minutos despues de que se complete la escritura y el usuario este de vuelta en el shell dando nuevas ordenes.

Todos estos factores y otros hacen vital que se tenga cuidado cuando se desconecte la maquina. Hay disponibles herramientas para ayudar con estas tareas y deberian ser utilizadas siempre que sea posible. Naturalmente la alimentacion de la maquina se ira inesperadamente; la alimentacion del edificio puede quedar interrumpida, por ejemplo. Versiones modernas del Unix pueden soportar tales caidas de potencia y desconecciones incorrectas, aunque con cierto riesgo de fallo para el sistema o de perdida de los contenidos del disco del sistema. Se pueden evitar tales problemas reduciendo la probabilidad de desconexiones inadvertidas al minimo posible.

Desconexion de la maquina.

En principio, una desconexión correcta advierte a los otros usuarios para que se despidan antes de que el sistema se pare, eliminara cuidadosamente todos los procesos no escenciales actualizara varios ficheros y registros, sincronizara el disco con los buffers en memoria, y finalmente eliminara el resto de los procesos. Algunos sistemas pueden estacionar automaticamente las cabezas del disco bajo software, como parte de la desconeccion. De hecho, algunas maquinas unix incluyen el conmutador de potencia controlado de modo que el ultimo paso del proceso de desconeccion es la desactivacion fisica de la maquina.

La orden Sutdown.

Pueden utilizarse varias herramientas para desconectar la maquina, y la utilizacion de cualquiera es preferible a desconectarla sin mas. La orden sutdown es la mas segura pero la mas lenta. La orden sutdown es un guion shell localizado en /etc/shutdown, y puede ser inspeccionada para entenderla mejor. Como todas las herramientas relacionadas con la activacion y desactivacion de la maquina, sutdown esta reservada al superusuario. Solo puede ser ejecutada en la consola de sistema, y solo desde el directorio raiz, si estas condiciones no se satisfacen sutdown se quejara y rehusara tomar acciones.

La orden sutdown fue pensada para ser interactiva con el usuario controlando las acciones tomadas durante el procedimiento de desconexion. La orden puede ser todavia ser utilizada interactivamente, pero las versiones recientes del sistema Unix permiten usar la opcion -y, que instruye a sutdown para que responda a las preguntas por si misma:
sutdown -y
Esta forma de oreden es mucho mas facil de utilizar que la orden sin la opcion -y. Antes de ejecutar esta orden, es cortesia verificar la actividad de los otros usuarios para asegurarse que no esten haciendo algo critico. Pueden utilizarse las ordenes who, ps -af para determinar la actividad actual del sistema. Ademas se deberia de comprobar que no haya trabajo en impresion ni transferencia de datos uucp enprogreso, ya que estas actividades volveran a empezar desde el comienzo tras un rearranque si son interrumpidas por la desconeccion. Cuando se ejecuta, sutdown advierte a todos los usuarios que la maquina se desconectara pronto y que se deberian despedirse. Algunos de estos mensajes son enviados a todos los usuarios en sesion del sistema, y otros estan limitados a la consola, el mensaje de aviso que comienza con “Broadcast Message ...” es enviado a todos los usuarios actualmente presentes en la maquina por la orden /etc/wall inmediatamente despues que comienza el proceso de desconexion. Luego sutdown hace una pausa de 60 segundos antes de continuar con el proceso, se espera que los usuarios respondan de forma inmediata, cierren cualquier fichero abierto,aseguren su sesion, y luego se despidan. Todos los usuarios (excepto root) deben tomar accion inmediatamente. Despues de estos mensajes sutdown detiene todos los procesos activos, actualiza el disco y paulatinamente lleva al sistema opertivo hasta su detencion. Finalmente, el sitema llega a un punto donde la potencia puede ser desconectada o puede iniciarse un nuevo arranque. Espere siempre el mensaje de “Reboot the System Now”; o su equivalente, antes de desactivar la potencia o volver a arrancar el sistema realmente para asegurarse que el proceso se ha realizado con exito.

Por omision sutdown permite 60 segundos entre el sistema de aviso y el comienzo efectivo de la secuencia de desconexion. Se puede cambiar este tiempo, con la opcion -g (grace), por ejemplo:
sutdown -y -g300
esperara 5 minutos despues del mensaje de aviso.

Existe un procedimiento de desconeccion mas rapido, cuando se sabe que la maquina esta en un estado de quietud, basicamente se requieren 3 acciones:

Los buffers del sistema deben de sincronizarse con el disco para que este quede actualizado.
Debera desmontarse cualquier sistema de ficheros adicional al sistema de raiz.

El marcados de sanidad del disco debe ser correcto, de modo que no sea necesaria la comprobacion de fichero cuando vuelva a arrancarse la maquina.

Para satisfacer estos requerimientos se utiliza:

sync, que actualiza el disco rigido. Normalmente se ejecuta 2 o 3 veces sucesivamente.
umount umountall para retirar con seguridad los ficheros adicionales.
uadmin con 2 segmentos. El primer argumento, 2, produce una desconeccion, y el segundo 1, o 2, hace que la maquina sea arrancada inmediatamente con una reinicializacion dura. Utilice el segundo argumento como 0 (cero) para desenchufar la maquina.

La Secuencia de Arranque.

Cuando se conecta la potencia de la maquina sigue un proceso de arranque. Esta secuencia de arranque (boot) puede tardar varios minutos dependiendo del hardware y software instalado en la maquina y no hay modo de hacer que vaya mas rapidamente. El proceso de arranque incluye varios chequeos de sanidad y con frecuencia trata de reparar cualquier daño, especialmente daños en los ficheros de disco rigido. La mayoria de las maquinas Unix tienen procedimientos internos para minimizar esta verificacion de errores si la desconeccion anterior se completo correctamente. Por tanto, la secuencia de arranque despues de una caida de potencia o de alguna otra desconexion inadvertida sera probablemente mas completa y compleja que un arranque despues que una desconexion normal. En cualquier caso, la secuencia de arranque suele ayudar a reparar los problemas del sistema. La primera respuesta a cualquier desbarajuste de la maquina deberia ser normalmente volverla a arrancar.

En el procedimiento de arranque, en primer lugar se ejecuta el cargador ROM, cuya responsabilidad es cargar las primeras partes del sistema operativo del disco. de hecho, el cargador ROM carga otro programa cuyo trabajo es cargar el propio sistema Unix. Este software adicional cargador esta almacenado en el disco del sistema, de modo que debe ser cargado por modulos hardware y ROM que existen permanentemente. Despues que el cargador software es traido a memoria, la ROM cede el control y este comienza a ejecutarse. En este punto la maquina esta obligada a ejecutar el sistema Unix ya que el cargador software solo puede tratar con su propio sistema operativo. Cuando el cargador

software comienza, muestra el mensaje:
Booting the UNIX System...
y carga entonces el nucleo (kernel) del sistema operativo, que es normalmente /unix. Se puede presionar una tecla mientras se visualiza el mensaje “Booting”, y el cargador permitira introducir el nombre del nucleo alternativo para cargar. Este nucleo alternativo debe residir in /stand/unix. Como parte de la secuencia de inicializacion, el nucleo puede visualizar cuanta memoria total real hay instalada en el sistema, si esta cantidad difiere de la cantidad de memoria fisica, debe haber un problema de hardware que deberia ser reparado. Como parte del proceso de inicializacion, el nucleo analiza las rutinas de dispositivo asociadas con tarjetas adicionales instaladas y los mensajes “Wangtek ...”, etc. aparecen es esta etapa.

Estados Init.

El procedimiento de arranque del sistema Unix se complica por la posibilidad de hacer entrar al sistema en diferentes estados, es decir, el sistema puede adoptar varios modos de operacion conocidos como estados init, debido a que /etc/init es el programa responsable del mantenimiento del sistema en funcionamiento correcto.

El estado mas comunmente utilizado es el modo multiusuario, este es el estado del sistema utilizado para casi todas las interacciones en estas notas y el unico que permite mas de un usuario. Otro estado historicamente utilizado pero de raro uso hoy, es el modo de usuario unico, este ultimo es una version de Unix de multitarea, por lo que permite multiples procesos, pero no multiples usuarios, este estado puede ser utilizado para una actualizacion del kernel (nucleo) del Unix rapida. Existen otros estados, la designacion de estos estados se muestra en la siguiente tabla:

Estado	Funcion
0	Desenchufar la maquina
1	Modo de usuario unico
2	Modo de multiusuario

3	Modo multiusuario con red
4	No usado
5	Desconexion a ROM (o desconexion y arranque)
6	Desconexion y arranque

Por omision shutdown lleva la maquina al estado 0, preparando asi la desactivacion de la potencia del sistema. Sin embargo el argumento -i permite establecer explicitamente el estado init a uno de los estados disponibles.
shutdown -y -g45 -i0
Suspendera el sistema, mientras que:
shutdown -y0 -i6
Volvera a arrancar la maquina. La mayoria de las versiones de shutdown solo soportan los estados init 0, 5 y 6.
Normalmente el sistema estara en el estado 2 a menos que se esten utilizando facilidades de la red, en cuyo caso se encontrara en el estado 3. La orden telinit sirve para cambiar entre estos estados operativos. Por ejemplo la siguientes orden activara la comunicacion por la red desde el estado 2:
telinit 3
Despues se puede regresar al estado 2 con la orden:
telinit 2

Tras la terminacion de la inicializacion interna, el sistema arranca el demonio /etc/init, el cual asume el control de arranque. El proceso init permanece activo durante todo el tiempo que el sitema este corriendo. Sirve varias funciones importantes, la mas importante es asegurarse que otros demonios del sistema esten en ejecucion cuando deban.

El proceso init obtiene sus instrucciones del fichero /etc/inittab (tabla de init). El contenido de este fichero controla todos los estados init y tambien determina que procesos deben ser regenerados cuando mueran. El fichero inittab es una base de datos tipica de Unix, por lineas formadas por varios campos separadas entre si por dos puntos “:”. Cuando init comienza lee las lineas de fichero inittab por orden toma una accion dependiendo del contenido de cada linea.

La estructura inittab es la siguiente:
El primer campo de cada linea es un identificador que designa a cada linea y que deberia ser unico.

El segundo campo define los setados init para los cuales la linea esta activa. Puede contener mas de un estado, como en 23, que define la linea como activa en los estados 2 y 3. Si no tiene contenido, esta linea estara activa en todos los estados init.
El tercer campo describe la accion que init tomara cuando se encuentre en uno de los estados indicados en el segundo campo. Estas acciones pueden ser:

off	Eliminar la orden designada si existe
Once	Ejecutar el proceso cuando entre al estado designado sin esperar a que se complete
Wait	Ejecutar el proceso cuando entre al estado designado esperando a que se complete
Boot	Ejecutar el proceso unicamente cuando init lee inittab en el tiempo de arranque, no esperando a que se complete el proceso
Bootwait	Ejecutar unicamente cuando init lee inittab en el tiempo de arranque, esperando a que se complete el proceso
Initdefault	Tiene significado especial y no incluye campo de orden
respawn	Iniciar el proceso cuando estre a los estados designados y lo regenere cada vez que detecte que init ya no esta ejecutandose.

Existen algunas lineas en la tabla inittab que especifican guiones que se ejecutan cuando se solicitan estados especificos. Todos ellos son guiones shell y pueden ser inspeccionados si se desea. Generalmente se ejecutara el /etc/rc2 (“run control” para el estado 2).

La tabla inittab solo puede ser modificada por el superusuario, quien puede por ejemplo cambiar la accion respawn por off para desactivar un proceso, o hacer el cambio inverso para reactivarlo. Observe que en muchos sistemas los cambios efectuados a inittab no sobreviviran a la adicion de nuevo hardware, por lo que debera actualizarse, con los cambios que se quieran, despues de una instalacion de hardware.

El programa init lee el fichero inittab solo una vez, cuando se inicia. Si se modifica inittab, estos cambios no tienen efecto hasta que se informe a init que el fichero ha cambiado. Esto se hace utilizando el programa telinit:
telinit q

Asi, init vuelve a leer inittab y toma acciones basadas en los cambios desde la ultima vez que la leyo, sin cambiar el estado init.

Hay otra accion importante asociada generalmente con el proceso de arranque. Se trata de la verificacion del sistema de ficheros. Como el sistema Unix depende tando de la sanidad del sistema de ficheros, existe una herramienta especial para verificarlo y repararlo. Se trata de la orden /bin/fsck (file system check), que esta reservada al super usuario. En tiempo de arranque, el guion /etc/bcheckrc de la inittab comprueba el indicador de sanidad del sistema de ficheros por si fue escrito como parte de la secuencia de desconexion. La orden uadmin escribira este indicador correctamente, no asi las desconexiones imprevistas. si el indicador no esta definido correctamente, el guion bcheckrc ejecutara automaticamente /etc/fsck.

La orden fsck tambien puede ser ejecutada en la consola del super usuario, con el nombre del sistema de ficheros a verificar como argumento. Es deseable ejecutar esta orden en un sistema de ficheros desmontado, ademas debera de especificarse el tipo de ficheros a verificar con la opcion -f.
La orden fsck ejecuta cinco fases diferentes:

1. Comprueba las tablas internas del tamaño real de los ficheros.
2. Verifica la sanidad de los nombres de camino de los directorios y de los ficheros.
3. Comprueba la conectividad correcta entre ficheros y directorios padre.
4. Verifica la cuenta de enlace entre ficheros y sus nombres para asegurarse que los ficheros sean correctamente diferenceados.
5. Asegura que todos los bloques no referenciados esten correctamente introducidos en la lista de libres del sistema de ficheros.

Cuando fsck encuentra un fichero o parte de un fichero que no esta correctamente vinculado en el sistema de ficheros, lo revincula al sistema en un lugar especial. este lugar son los directorios /lost+found y /usr/lost+found si la maquina tiene dos sistemas de ficheros. El directorio /lost+found tambien aparecera en discos flexibles que contengan el sistema de ficheros.

El Super Usuario

El administrador del sistema o superusuario, es generalmente us usuario individual y responsable de mantener el sistema en ejecucion correctamente. A travez del tiempo se ha llegado demostrar que una sola persona puede mantener la consistencia de un sistema mucho mejor que varios usuarios. El administrador del sistema se convierte en el punto de contacto para las peticiones de otros usuarios y tiene la responsabilidad de mantener la maquina en una correcta ejecucion. En una maquina Unix personal pequeña el propietario es normalmente el administrador del sistema que da acceso a otros usuarios, hace copias de seguridad de los ficheros de disco, etc. En un sistema multiusuario el administrador tambien debe de actuar como policia y como bombero, manteniendo la maquina en buenas condiciones para beneficio de los otros usuarios.

El shell proporciona un introductor (prompt) especial para recordad que el que se esta activando es el superusuario, se trata de # . El directorio propio (PATH) del superusuario o root es el directorio raiz, / (diagonal). El id de presentacion root obtiene servicios del perfil al igual que un usuario normal, y se puede crear o modificar el fichero /.profile para personalizar este entorno. En maquinas modernas el uso de id de presentacion de root esta limitado a la consola del sistema a menos que se efectuen arreglos especiales en el /etc/default/login, o bien se puede entrar con un id de presentacion de usuario y despues cambiar al modo de super usuario con su (switch user).
Se puede utilizar su para cambiar a cualquier otro id de presentacion por omision que utiliza su.

```
$ su
Password:
#
```

Mientras su esta en ejecucion, el usuario tiene privilegios de administracion completos sobre el sistema, para regresar solo hay que presionar Ctrl-D o escribir exit.

```
$ su
Password:
```

```
# exit
$
```

Lo que se hace en este caso es hacer uso de un subshell sobre el shell de presentacion, y cualdo se termina con su se regresa al entorno normal.

Programa del Administrador “Sysadmsh”

En la version Unix del OPEN DESKTOP el agente de usuario se llama sysadmsh (system administration shell), este agente no esta restringido a ser corrido solo por el super usuario, sino puede ser ejecutado por cualquier usuario. Sin embargo, cuando es ejecutado por un usuario normal, restringe sus acciones a las que son permitidas por ese usuario en particular. Al tratar de hacer una accion no permitida se obtiene un mensaje como el siguiente:

> Menu access denied -
> Backup command authorization required.
>
> Press <Return> to continue.

Ahora vamos a ver las opciones principales del sysadmsh asi como lafuncion que tiene cada una de ellas y sus subopciones.

SYSTEM	Administrar y configurar los recursos del sistema y reportar sobre el estado del mismo. *Report Configure Hardware Software Audit Execute Terminate*
BACKUPS	Realiza backups de archivos, sistema de archivos y al sistema completo. *Create Restore Schedule View Integrity*
ACCOUNTS	Administrar informacion de acceso a terminales y las cuentas de los usuarios. *User Defaults Terminal Report Check*
PRINTERS	Administrar el sistema de impresion. *Configure Schedule Request Auxiliary Priorites*
MEDIA	Copiar, comparar, leer y formatear discos flexibles y cintas. *List Extract Archive Format Duplicate Tapedump*

JOBS	Reportar, autorizar y terminar trabajos *Report Terminate Authorize*
DIRS/FILES	Examinar, manipular, modificar y guardar discos y directorios. *List View Copy Edit Modify Print Archive Differences Remove UseDos*
FILESYSTEMS	Checar, montar, desmontar, adicionar y crear sistemas de archivos. *Check Mount Unmount Add Floppy DOS Quit*
QUIT	Salir del shell de administracion del sistema. Sin Opciones

Ahora detallemos las subopciones de cada una de estas opciones a continuacion.

SYSTEM:

REPORT	Reporta sobre el estado actual del sistema. *Activity Users Printers Disk Network Messages Software*
CONFIGURE	Configurar los archivos del sistema. *Security Kernel Logout Defaults International Network Time*
HARDWARE	Adicionar o remover hardware del sistema. *HardDisk Tape Printer Card_Serial Mouse Video*
SOFTWARE	Adicionar o remover un paquete de software del sistema. *Install Remove List Quit*
AUDIT	Administrar y examinar la informacion de auditoria del sistema. *Eneable Diseable Colletion Report Files*
EXECUTE	Ejecutar programas que son especificos del sistema. *Sin* Opciones
TERMINATE	Dar de baja el sitema para poder desconectar la maquina. *Sin* Opciones

BACKUPS:

CREATE	Crear Backups *Schedule Unsuchedule*
RESTORE	Restablecer el sistema de ficheros y ficheros *Partial Full*
SCHEDULE	Editar el archivo de bitacora para modificar frecuancia de respaldo programada.
VIEW	*Sin* Opciones
INTEGRITY	Ver el contenido de respaldo *Sin* Opciones

ACCOUNTS:

USER	Parametros especificos de cuentas. *Examine Create Retire*
DEFAULTS	Parametros por omision (default) del sistema completo. *Authorization Password Logins*
TERMINAL	Administrar la entrada en la base de datos de terminales. *Examine Create Delete Lock Unlock Assign*
REPORT	Producir reportes sobre la expiracion de passwords, terminales y actividad del login. *Password Terminal Login*
CHECK	Revisar los contenidos de los archivos tcb para verificacion de errores. *Databases Password*

PRINTERS:

CONFIGU	Configurar impresoras para el servicio lp.

RE	*Add Modify Remove Default Parameters Errors Content Users*
SCHEDULE	Arrancar / Parar el servicio lp y manejo de impresoras. *Begin Stop Accept Reject Eneable Diseable*
REQUEST	Mover o cancelar requerimientos en el servicio de impresora lp. *Move cancel*
AUXILIARY	Administrar ruedas de impresion, filtros y formas preimprentas. *Alert Filter Pforms*
PRIORITIES	Fijar la prioridad de las colas de impresion. *Default Highest Remove List*

MEDIA:

LIST	Listar el contenido de un floppy o de una cinta. Sin Opciones
EXTRACT	Extraer el contenido de un floppy o de una cinta. Sin Opciones
ARCHIVE	Almacenar ficheros, directorios y/o sistemas de archivos en algun medio de almacenamiento (media). Sin Opciones
DUPLICATE	Hacer una copia de un floppy o de una cinta. Sin Opciones
TAPEDUMP	Mostrar el contenido fisico de una cinta. Sin Opciones

JOBS:

REPORT	Reportar sobre los procesos actuales.

	Sin Opciones
TERMINATE	Terminar un proceso no deseado que esta corriendo. Sin Opciones
AUTHORIZE	Autorizar a los usuarios el correr trabajos. *Schedule Delayed Environment*

DIRS/FILES:

LIST	Listar los ficheros del directorio actual. Sin Opciones
VIEW	Ver el contenido de un fichero. Sin Opciones
COPY	Copiar un fichero. Sin opciones
EDIT	Editar uno o mas ficheros. Sin opciones
MODIFY	Modificar un fichero. Sin Opciones
PRINT	Imprime ficheros. Sin opciones
ARCHIVE	Almacenar ficheros. Sin Opciones
DIFFERENCES	Comparar dos o mas ficheros. Sin Opciones
REMOVE	Borrar ficheros o directorios. Sin Opciones
UseDOS	Utilizar utilerias DOS para manipular ficheros DOS. Sin Opciones

FILESYSTEMS:

CHECK	Checar y reparar inconsistencias en un sistema de ficheros. Sin opciones
MOUNT	Montar un sistema de ficheros. Sin opciones
UNMOUNT	Desmontar un sistema de ficheros. Sin opciones
ADD	Adicionar informacion apropiada para un nuevo sistema de ficheros. Sin opciones
FLOPPY	Crear un sistema de ficheros en un disco floppy Sin opciones
DOS	Adicionar el soporte para el sistema de ficheros DOS. Sin Opciones

Administracion de las cuentas de Usuario

Las cuentas de usuario ayudan al administrador a darse cuenta la operacion que se esta llevando por parte de las personas que estan en el sistema, ademas de que ayuda a controlar los recursos del mismo. Cada cuenta tiene su propio “login name” (nombre d entrada), el cual es unico, y “password” (contraseña de entrada), con estos el usuario tiene derecho a ingresar al sistema, y un “home directory” (directorio de trabajo) donde el usuario lleva acabo sus labores. Ademas el sistema tiene ciertos defaults que define cuanto tiempo durara el password, si se les permite escoger a los usuarios su propio password, y cuantas veces puede equivocarse al tratar de entrar al sistema, antes de bloquear la entrada.

El administrador del sistema crea las cuentas para los usuarios, y mantener estas cuentas cambiando los passwords, los grupos, y los parametros de las cuentas cuando sea necesario.
En esta parte dek curso analizaremos los siguientes puntos:

Accounts-Administracion de cuentas: add (adicionar), alter (alterar) y remove (borrar), asi como crear grupos de usuario.
Configuracion default de cuentas: configurar los parametros de default de password y login.
Administracion del login de la terminal: realizar reportes de login de los usuarios, de uso de la terminal, y de estatus de password.

Es importante señalar que no se recomienda editar los archivos /etc/passwd con un editor de texto, existen versiones donde esta operacion se puede realizar, pero no es recomendable ya que no es un metodo muy confiable. Una mala manipulacion puede causar mensajes de error y puede causar que el sistema no acepte los logins. Para realizar este tipo de operacion existe el programa “sysadmsh”.

ADMINISTRACION DE CUENTAS

Creando un Usuario.

Se puede dar de alta un usuario en el sistema con el programa sysadmsh, el cual se encarga de crear una nueva entrada a la base de datos Accounts. La base de datos contiene informacion sobre el nuevo usuario (como el login name y el password inicial) que el sistema utiliza para dejar al usuario trabajar. El sysadmsh crea un "home directory" para el usuario, una caja de correo para ser usada con el comando mail, y un archivo de inicializacion.
Para crear una cuenta de usuario, siga los siguientes pasos en el menu del sysadmsh:

Accounts -> User -> Create

Siga los siguientes pasos para adicionar un usuario:

1. Llene el campo "username" (nombre de usuario) y si lo desea el campo de "comment" (comentarios).
2. Si desea alterar los defaults, seleccione "Yes" y defina los campos que se muestran en la siguiente seccion, "Alterando los defaults de usuario". Llene cada campo como sea necesario, presione F3 para escoger de las listas de valores disponibles. cuando se presione Return, el campo esta llenado con la informacion que se ingreso.
3. Cuando se sale de la forma, una ventana aparecera para que confirme la informacion que se ingreso. Si confirma, una serie de mensajes de creacion son mostrados de la siguiente manera:
   Created home directory: pathname
   Created shell file: filename
   Greetings mail sent to user: name
   Esto indica que todos los archivos y directorios necesarios han sido creados, esta informacion default es tomada del archivo /usr/lib/mkuser
4. En el siguiente paso el sysadmsh le preguntara si ha creado un passsword inicial; las posibles selecciones para "Asign first password" son las siguientes:

Now	asigna a la nueva cuenta un password
Later	no asigna a la nueva cuenta un password (el usuario no podra entrar)
Blank	asigna a la nueva cuenta un password vacio (se le pedira al usuario ingresar el password en la primera entrada)

Remove	no asigna a la nueva cuenta ningun password en absoluto (el usuario puede entrar sin ningun password)

Si usted selecciono generar un password para el nuevo usuario vera las siguientes 2 opciones:

1. Pick up your own password
2. Pronunceable password will be generated for you

5. Si usted selecciono la primera opcion le indica al sistema que usted ingresara su propio password; se le pedira que teclee el password en dos veces.
6. Si selecciono la segunda opcion el sistema creara un password para usted; el password generado es mostrado con su version separada por silabas. La separacion silabica en silabas pronunceable esta diseñada para ayudar a la memorizacion del password.
7. Dar el nuevo password al usuario. Si se selecciono el forzar el cambio del password, se le pide al usuario que cambie el password inmediatamente despues de la primera entrada al sistema.

La nueva cuenta esta ahora lista para ser utilizada, y se mantendra de acuerdo a los parametros de default de la seguridad a menos que se haya especificado valores particulares para el usuario.

Alterando los valores default de la creacion de cuentas.

Para llevar acabo esta operacion seleccione "Modify Defaults", despues usted apreciara una forma en pantalla, en esta apreciara que el cursor estara posicionado en el campo de "Login group". Algunos de los campos pueden ser modificados al momento de crear la cuenta del usuario en el modo de modificacion, estos campos son solamente informacionales; sus valores pueden ser cambiados. Estos campos son los siguientes:

Login group	El grupo asociado con la cuenta cuando el suario entra. Este campo puede ser cambiado, pero no debera estar vacio. Este campo es el grupo del usuario en /etc/passwd. Presionando F3 se muestra una lista de los grupos existentes.
Groups	Los grupos en los que este usuario es un miembro.
Login shell	El shell que el usuario utilizara, el valor default esta definido en el archivo /etc/default/authsh. Si la ruta completa es ingresada, el shell descrito por esta ruta es simplemente el usado como el shell usado por el usuario. Sin embargo si no se especifica la ruta, se asume que se trata del shell predefinido, es decir, el shell que se encuentra en el subdirectorio /usr/lib/mkuser.

Home directory	Define donde residiran los archivos de usuario. La opcion del directorio default se enfatiza; presione Return para seleccionar el directorio de default. Las opciones del directorio de trabajo son las siguientes: • *Create:* Crea un nuevo directorio para el usuario • *Do not create:* no crear un directorio para el usuario • *Populate existing:* use el directorio especificado existente Mas adelante analizaremos usuarios que comparten directorios de trabajo.
User ID	Es el numero de identificacion del usuario (ID). Una vez seleccionado un numero de identificaion, este no puede ser cambiado porque podria causar inconsistencia en la auditoria del sistema.
Type of user	En la mayoria de los casos el tipo de usuario es “individuo” o “pseudo-usuario”. Por default este campo asume el valor “individuo” que identifica a la gente real con nombres. Los usuarios “pseudo-user” son cuentas anonimas dedicadas a ciertas tareas administrativas del sistema.
Account that may su to this user	Se refiere al usuario responsable de esta cuenta. Este campo puede ser cambiado si y solo si el usuario no es un individuo. para usuarios individuales este campo esta vacio, pero para usuarios no individuales no debera de estar vacio. por ejemplo, la cuenta de root debera tener el nombre del usuario responsable de la cuenta. Presione F3 para ver la lista de los usuarios del sistema.

Compartiendo directorios de trabajo.

Se puede crear cuentas que compartan el mismo directorio de trabajo (login directory); para hacer esto, se crea el directorio normalmente durante la adicion de un nuevo usuario. Usted deberia despues de salir del sysadmsh e introducir los siguientes comados (reemplazando homedir con el nombre real del directorio).

cd homedir
chmod 775
chown aunth

Ademas, introducir uno de los comandos siguientes deacuerdo al shell de login usado para la cuenta:

Bourne o Korn shell
chmod 660 .profile
chmod 660 .kshrc (korn shell solamente)
C-shell
chmode 660 .login .chsrc

Esto asegura que los mienbros del mismo grupo de login puedan compartir este directorio. Note que si usted asugna diferente grupo de login de varios usuarios, estos no podran compartir el directorio.

Alterando los valores default mostrados para las cuentas de usuario.

Usted puede alterar las selecciones default que aparecen en el menu de creacion, editando el archivo /etc/default/authsh. Los valores default siguientes pueden ser definidos:

login group
groups
login shell
home directory
range of user IDs
type of user

Alterando o asignando autorizaciones de usuario.

Las autorizaciones son asignadas solo a usuarios confiables con la administracion de los subsistemas. Para asignar una nueva autorizacion a un usuario, se hace la siguiente seleccion en el sysadmsh:

Accounts -> User -> Examine: Privileges

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion de privilegios.
Despues de esto se desplegara la forma. Usted puede presionar F3 para desplegar una lista con las autorizaciones disponibles.

Eliminando una cuenta de usuario.

En el sentido estricto, un usuario nunca sera borrado del sistema. Una identificacion de usuario (user ID), una vez asignada nunca sera reusada. En lugar de esto una cuenta es “retirada” o “removida” de servicio. Para retirar una cuenta de usuario, haga la siguiente seleccion en el sysadmsh:

Accounts -> User -> Retire

Una cuenta que es retirada nunca podra ser reactivada, ya que el retiro es permanente. Al retirar una cuenta de usuario no se borran los archivos de usuario; el administrador del sistema debe hacer esto manualmente.

Bloqueando y desbloqueando una cuenta de usuario.

El administrador del sistema puede bloquear una cuenta para evitar su uso. Ademas de que una cuenta se bloqueara automaticamente si los parametros del login han sido excedidos. Una vez que un usuario o una terminal es bloqueada, solo el administrador puede desbloquear esta cuenta o terminal. Para hcer el bloqueo de una cuenta o terminal, haga la siguiente seleccion en el sysadmsh:

Accounts -> User -> Examine: Logins

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion del login.

A continuacion se mostrara una forma, en la cual se podra posicionar en la casilla “Lock status” y seleccionar “Apply Administrative lock” o “Clear All Locks” segun lo desee.

Cambiando el grupo de un usuario.

Para cambiar el grupo del usuario siga los siguientes pasos en el sysadmsh:

Accounts -> User -> Examine: Identity

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion de la identidad.

Cambiando el directorio de trabajo de un usuario.

Usted puede cambiar el directorio de trabajo de un usuario ademas de sus archivos, siguiendo los siguientes pasos en el sysadmsh:

Accounts -> User -> Examine: Identity

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion de la identidad.
Al desplegarse la forma en pantalla usted se podra posicionar en la casilla del directorio de trabajo "Home Directory", y podra seleccionar lo siguiente:

Keep	no hace cambios al directorio principal para este usuario.
Edit	cambia la ruta del directorio principal del usuario, pero no mueve ningun archivo.
Create	crea el directorio principal para este usuario.
Move	Renombra el directorio principal del usuario, moviendo todos los archivos del anterior directorio al nuevo.
Restore	Cambia la ruta a su valor anterior sin mover ningun archivo.

Cambiando un password o los parametros del password de un usuario.

Un administrador puede cambiar el password de un usuario en cualquier momento. Para hacer esto se hace el siguiente seguimiento en el menu del sysadmsh:

Accounts -> User -> Examine: Password

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion del password, una forma se mostrara.
Los siguientes parametros definen las restricciones de password por usuario:
- *Password required*
Si esta la opcion "Yes" significa que el usuario podra entrar sin la necesidad de ningun password, por el contrario si esta la opcion "No" debera de existir un password para permitir el login.
- *User can choose own*
Este parametro determinara si los usuarios pueden escoger su propia contraseña. Si este parametro es

seleccionado como “Yes”, se le permite al usuario escoger su password; por el contrario si esta un “No”, el sistema debera de generar la contraseña.
- *Maximun generated password lenght*
Indica la longitud maxima del password generado por el sistema. El valor maxomo es de 80 caracteres.
- *Checked for obviousness*
Este parametro indica si el sistema debera de correr chequeos de trivialidad para el nuevo password. Estos chequeos aseguran que el password no aparece en el diccionario en linea y los otros cheques descritos en goodpw.
- *Current password status*
Esta opcion tiene las siguientes subopciones:

Keep no cambia el password
Change invoca el procedimiento de cambio
Disable deshabilita el password, el cual bloquea efectivamente al usuario
Remove borra el password, premitiendo al usuario entrar sin ningun password
Aun root no puede cambiar el password si el minimo de intervalo de tiempo ha expirado.
- *Change password at login*
Esta opcion le permite forzar al usuario a cambiar su password en la proxima vez que entre en sesion.

Alterando los parametros de expiracion del password del usuario.

Algunas veces es util definir los parametros de expiracion del password de un usuario que difiere de los defaults del sistema. Para hacer esto haga lo siguiente:

Accounts -> User -> Examine ->: Expiracion

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion de la expiracion.
El tiempo de vida del password esta dividido en tres intervalos:

El password es valido
El password ha expirado; el usuario puede estar aun en sesion y cambiarlo

El password esta muerto; el usuario esta bloqueado y el administrador debera de bloquear la cuenta y el usuario debera de cambiar el password
Para desanimar a los usuarios para cambiar su password cuando este expira e inmediatamente cambiarlo al que ellos recuerdan, el sistema tambien almacena un minimo de tiempo entre cambios de password. El esquema del tiempo de vida del password se implementa como sigue:
Minimum number of days between password changes El numero de dias que un usuario debera esperar antes que pueda cambiar su password.
Maximun numbers of days before password must be changes Define el periodo de tiempo que un password es valido.
Maximun numbers of days before account is locked for not Define el intervalo entre el ultimo cambio de password y cuando el password muere.

Cambiando los parametros de auditoria del usuario.

Usted puede definir los parametros de auditoria de usuarios individuales igual que se hace con los parametros del sistema. Cualquier seleccion definida para un usuario se sobrepone a los valores default del sistema. Para definir o cambiar los parametros de auditoria del sistema, se hace la siguiente seleccion en el sysadmsh:

Accounts -> User -> Examine: Audit

Los dos puntos indican que se debe de llenar el nombre de usuario antes de escoger la seleccion de la auditoria.
Existen tres posibles valores para cada evento de los mostrados en el display:

Default usa los valores default de las cuentas del sistema
Always siempre hace auditoria de este evento, se sobrepone al valor default del sistema
Never nunca hacer auditoria de este evento, se sobrepone al valor default del sistema
Se puede presionar la tecla F3 para seleccionar de una lista los posibles valores, o se puede teclearlos directamente. Se reconocen las abreviaciones por ejemplo ‘n’ significa “nev”, y ‘N’ significa “never”. Para ejecutar la forma, presione Ctrl-x.

Adicionando o cambiando grupos.

Para adicionar un grupo, introduzca un nombre de un grupo nuevo cuando se esta creando o alterando una cuenta de usuario. El sistema le indicara que el grupo no existe, entonces se le pedira que confirme la creacion del nuevo grupo.

Cambiando el numero maximo de grupos suplementarios.

Los grupos suplementarios son aquellos distintos del conjunto basico definido en /etc/group. por default, el numero maximo de grupos suplementarios es 8. Este numero es controlado por el parametro "sincronizable" del kernel llamado NGROUPS. Este valor puede ser cambiado utilizando el sysadmsh de la siguiente forma:

System -> Configure -> Kernel -> Parametres

Y seleccionando la categoria 3, "Files Inodos, and Filesystems", y cambiando el valor de NGROUP. El Kernel debera de ser reencadenado y arrancado nuevamente para que el nuevo valor sifra efecto. Use el sysadmsh para reencadenar el kernel de la siguiente manera:

System -> Configure -> Kernel -> Rebuild

Administracion de las cuentas de Usuario

CONFIGURACION DEFAULT DE CUENTAS

Esta seccion explica como alterar los valores default de seguridad del sistema, los cuales incluyen el esquema de password default, las autorizaciones de los subsistemas y el numero de intentos login permitidos a los usuarios.
El sisteme esta preconfigurado con los valores y define el esquema de seguridad usado para las cuentas. La siguiente tabla muestra estos defaults, incluyendo los valores relajados (relaxed).

Valores default de seguridad relajados.

Parametros de Seguridad	Relajados	C2
Passwords		
Numero minimo de dias entre cambio	0	14
Tiempo de expiracion (dias)	infinito	42
Tiempo de vida (dias)	infinito	365
El usuario elige su propio password	yes	yes
El usuario puede correr el generador de passwords	yes	yes
Longitud maxima generada	8	10
Chequeo de passwords “obvios”	no	no
Password requerido para el login	no	yes
Password requerido para usuarios individuales	yes	yes
Logins		
Maximo numero de intentos sin exito (cuenta y terminal)	99	5
Pausa entre intentos de login (segundos)	0	2
Tiempo para completar el login (segundos)	60	40

Audit Event Types	none	A,B,F,H,I, J,K,L,M,N,Q,R,S,T
Authorizations		
Subsystem	queryspace, printerstat, printqueue, mem, terminal, audittrail, su	queryspace, printerstat, printqueue,
Kernel	execsuid, chmodsugid, chown, nopromain	execsuid, chown, nopromain
Default umask*	22	77

**Estos estan en /etc/profile y /etc/shrc. Una umask de 077 dice que la creaciond e archivos que son legibles solo por el dueño. Cuando se selecciona "relaxed", el valor de umask no es cambiado si el valor habia sido previamente alterado.*

Seleccionando los valores de seguridad C2 default.

Despues de seleccionar los valores "relaxed", es posible regresar a los valores default del nivel C2, sin embargo esto no significa que su sistema automaticamente se configura a los requerimientos de un sistema C2, por definicion, un sistema C2 se debe aderir a los requerimientos de instalacion inicial. Para establecer los valores default C2, use la tabla anterior como una guia para reestablecer nuevamente los valores usando:

Accounts -> User -> Examine
Y seleccionar cada categoria.

Cambiando los parametros de seguridad dinamicamente.

Los siguientes parametros de cuentas del sistema pueden ser modificados:

autorizaciones
password
logins
Los parametros de seguridad del sistema controlan la manera en que los usuarios entran y, una vez que establecen una sesion, la terminal y el ambiente de autorizacion que el sistema les presenta.
usted deberia usar las funciones del sistema para definir su propia conducta del sistema default. Despues usar las funciones especificas del usuario para ajustar cualquier comportamiento para cualquier usuario con diferentes comportamiento para cualquier usuario con diferentes requerimientos. Como podria esperar, las entradas especificas del usuario se sobreponen a los valores default del sistema para un usuario dado.

Cambiando las restricciones de default del login.

La mayoria de los parametros que pueden ser fijados en los defaults del sistema tratan con la manera como un sistema crea una sesion de login. Estos incluyen logins particulares, y la manera de como los passwords son generados y exigidos. Los parametros de logins forzan las caracteristicas del bloqueo terminal y de cuenta. Cuando el usuario entra en sesion debe dar el login, y su password. Ademas el usuario tiene un numero limitado de intentos fracasados para entrar. Hay un numero limitado de veces que un intento fracasado de login puede ocurrir antes que sea la cuenta o terminal bloqueada. Si alguna de esas cuentas es exedida, el usuario o la terminal es bloqueado para futuros logins. Esta caracterisitca evita intentos de penetracion por parte de usuarios maliciosos.
Para accesar los parametros de restriccion de login, haga la siguiente seleccion en el sysadmsh:

Accounts -> Defaults -> Logins

Los parametros que describe la forma mostrada en el display son:

Maximum number of unsucceddful attempts before locking:
Este es el numero de intentos fracasados permitidos a los usuarios y terminales. Si un usuario en particular necesita un numero de intentos mas restrictivo o mas permisivo, la cuenta del usuario puede ser modificada o la configuracion de la terminal puede ser cambiada.
Delay (in seconds) between login attempts on terminal:
Este parametro controla el tiempo que debera de pasar entre intentos de logins fracasados. Para reducir

aun mas la restriccion de penetracion, el sistema puede hacer una pausa entre intentos de logins para incrementar el tiempo que toma tratar repetidamente de entrar al sistema.
Time (in seconds) to complete succesful login:
Este parametro determina cuanto tiempo tiene un usuario para introducir su nombre y password antes que el intento de login sea terminado.
CPU scheduling priority after succesful login:
Aqui se selecciona el valor asociado con nice de los procesos del usuario.

Cambiando las restricciones default de password.

Dado que puede controlar el numero de intentos que un usuario puede tratar para adivinar el password, la tarea es controlar la complejidad del password. Para accesar los parametros de default del password, siga las siguientes opciones en el menu del sysadmsh:

Accounts -> Defaults -> Password

En la forma mostrada en la pantalla se muestran los parametros que controlan los tipos de chequeo del password que le sistema hace. Estos parametros controlan el tiempo que un password es valido, y los procedimientos para cambiar el password de una vez que se vuelve invalido. Un password expira cuando su periodo de expiracion se cumple, El tiempo de expiracion puede ser seleccionado desde el sysadmsh para todo el sistema o para el usuario. Un password muerto causa que la cuenta del usuario sea bloqueada. Solo el administrador puede desbloquear la cuenta, la cual es tratada despues como una cuenta con un password expirado.
Para desanimar a los usuarios de cambiar su password cuando expira y despues cambiarlo inmediatamente, el sistema tambien almacena un tiempo minimo entre cambios de password. El password de un usuario no puede ser cambiado hasta que el tiempo minimo ha sido excedido. Este parametro tambien puede ser seleccionado para todo el sistema o para un solo usuario:.
Los siguientes parametros definen las restricciones de password:

Minimun days between password changes
Expiration time (days)
User can choose own
User can run generator

Maximun generated password length
Chequed for obviousness
Password requered to login
Single user password require
Cuyo significado resulta facil de entender de acuerdo a las secciones precedentes.
Cuando una cuenta es bloqueada por el sistema, solo root o el administrador de cuentas puede desbloquearla. El password debera ser cambiado entonces. Usted puede sobreponer estos parametreos para cualquier usuario como se describio en la seccion anterior.

Cambiando las autorizaciones de default.

El sistema define dos tipos de autorizaciones: Las autorizaciones del kernel y las autorizaciones del subsistema. Las autorizaciones del subsistema estan asociadas con los usuarios y les permite ejecutar utilerias. Las autorizaciones del kernel estan asociadas con los procesos y les permite a un proceso realizar ciertas acciones si el proceso tiene la autorizacion requerida. Cada sesion de usuario, tiene una serie de autorizaciones de kernel y el conjunto de autorizaciones del subsistema.
Para accesar los parametros de autorizacion, haga el siguiente seguimiento en el menu del sysadmsh:

Accounts -> Defaults -> Authorizationes

Usted apreciara un display, por el cual se movera presionando la tecla Tab, entre las autorizaciones del kernel y la de los subsistemas. Use la tecla F3 para ingresar a una ventana con la lista de cada conjunto de autorizaciones. La descripcione de las autorizaciones de subsistema son las siguientes:

Authoritation	Subsystem	Powers
mem	Memory	Acceso a los datos “privados” del sistema, listando todos los procesos del sistema
terminal	Terminal	Uso no restringido del comando “write”
lp	Line Printer	Administracion de la impresion
beckup	Backups	Realizacion de respaldos
auth	Accounts	Administrador de cuentas: adicion de usuarios, cambio de password, etc.
audit	Audit	Administrador de auditoria: corre la auditoria del sistema y genera

		resportes
cron	Job Scheduling	Controla el uso de los comandos cron, at y batch
sysadmin	System Integrity	Habilidad para correr el programa integrity

Las autorizaciones del subsistema determina el rol de administrador que un usuario puede asumir corriendo las utilerias permitidas. A un usuario general del sistema, no se le permiten autorizaciones del subsistema. Al staff administrativo se le proporcionan autorizaciones del subsistema basados en sus propias responsibilidades; esto es, al administrador de las cuentas se le da la autorizacion *auth* y al administrador de las impresoras se le da la utorizacion *lp*.

En la base de datos de los valores default del sistema, un conjunto default de autorizaciones es dado a todos los usuarios que no tienen autorizacion en la informacion especificada de la cuenta. En el caso de los valores default de C2, las autorizaciones del subsistema en la base de datos de los defaults del sistema esta vacia y las entradas especificas del usuario estan basadas en los roles administrativos, si existen, de ese usuario.

Las autorizaciones del subsistema sysadmin controla la facultad de correr el programa integrity, el cual checa los permisos de los archivos listados en la base de datos de control de archivos.

Las autorizaciones secundarias permiten accesos limitado por usuarios a los recursos que serian de otra manera controlados extrictamente. Estas autorizaciones proveen una conducta que es mas consiente con otros sistemas operativos UNIX. Esta es la tabla de las autorizaciones secundarias:

Autorizacion Secundaria	Subsystem	Descripcion
auditrial	audit	habilidad para generar auditoria personal sobre las actividades propias
queryspace	backup	uso del comando df para preguntar sobre el espacio en disco
printqueue	lp	Ver todos los trabajos de la cola usando lpstat
printerstat	lp	usar los comandos eneable/disable
su	auth	acceso a root, se requiere password para ingresar

Superusuario vs. administradores autorizados.

La mayoria de los poderes normalmente ejercidos por el superusuario en un sistema menos seguro estan asignados en los subsistemas de proteccion discutidos anteriormente. Sin embargo, algunas funciones todavia necesitan ser hechas por el usuario root. La autorizacion su permite a un usuario administrativo hacer un su (cambio de cuenta) a la cuenta del super susuario, pero no le garantiza el conjunto de autorizaciones root, el conjunto de autorizaciones del usuario estara todavia vigente.
Al superusuario se le pide que realice las siguientes tareas:

instalacion de software
particion del disco y mantenimiento del sistema de sistema de archivos
restauracion de archivos, recuperacion y seleccion de permisos
apagado del sistema
solucion de problemas

Autorizacion del Kernel

Estas autorizaciones gobiernan el poder de que los usuarios ejecuten servicios del sistema operativos especificos. por ejemplo la habilidad de cambiar de dueño a un archivo, es gobernado por la autorizacion chow. Las autorizaciones default del kernel son utilizadas cuando las autorizaciones del kernel del usuario no se especifican. Asi los usuarios que necesitan mas autorizacion pueden tener entradas especificas del usuario que les garantiza esas autorizaciones, mientras que los susarios normales pueden tener sus autorizaciones seleccionadas a los valores default del sistema.
Las autorizaciones del kernel son las siguientes:

Autorizacion	Accion
configaudit	Configura los parametros de auditoria del subsistema
writeaudit	Escribe los registros de auditoria
execsuid	Habilita para correr programas UID
chmodesugid	Habilidad para fijar el bit UID y el bit GID de los archivos
chown	Habilidad de cambiar el dueño de un objeto
suspendaudit	Suspender la auditoria del proceso

Autorizaciones del Kernel y usuarios administrativos.

Se deben asignar autorizaciones de kerner con autorizaciones de subsistema. A pesar de que muchas

de estas estan asignadas por default, se listaran en la siguiente tabla en caso de que se quiera modificar el valor default. Una exepcion es el subsistema de auditoria el cual requiere la audicion las autorizaciones configaudit y suspendaudit. Estas autorizaciones nunca deberian de ser asignadas por default, o a usuarios ordinarios. Otra exepcion es la autorizacion del sysadmin, la cual requiere la autorizacion del kernel chmodsugid, a pesar de que es mas simple correr el programa integrity como root.
Estos son los requerimientos de autorizacion del subsistema kernel:

Subsystem Authoritation	Autorizacion del Kernel requerida
audit	configaudit, suspendaudit, execsuid
auth	chown, execsuid
backup	execsuid
lp	chown
cron	execsuid, chown, chmodsugid
sysadmin	execsuid, chmodsugid, chown

Bloqueando o desbloqueando una terminal.

Para llevar acabo este proceso, siga las siguientes opciones en el sysadmsh:

Accounts -> Terminal -> Locks (esta opcion es para bloquear)
Accounts -> Terminal -> Unlock (con esta opcion se desbloquea)

Cuando aparece el prompt para la terminal, introduzca el nombre, por ejemplo: tty01. Cuando una terminal esta bloqueada, se muestra el siguiente mensaje al tratar de entrar a sesion:

```
Terminal is disabled—See Authentication Administrator
```

Configurando la base de datos de equivalencia de dispositivo.

El proposito de esta base de datos es almacenar los dispositivos terminales que son fisicamente los mismos, pero que son referenciados por diferentes rutas (ellos estan ligados, o son el mismo dispositivo con o sin control de modem, etc.). Este mapeo de equivalencias es muy importante en el caso de terminales, donde se asegura que la historia del login y el bloqueo de terminales se aplica

correctamente a cualquier ruta del dispositivo que el sistema ve.
Un ejemplo es alguien que deshabilita tty1a y despues habilita tty1A, debido que en los registros de la base de datos, esta registrada la equivalencia de estos dispositivos, se mantiene, por ejmplo, la cuenta de login fracasados. Otra vez el sistema hace esto automaticamente con los dispositivos que reconocen por default. Cualquier nodo de dispositivo creado para hardware inusual o software tiene que se r configurado y adicionado manualmente. Usted deberia de hacer esto si la documentacion le dice que lo haga o si usted sabe la operacion que esta realizando.
Para cambiar una entrada de asignacion de dispositivo, seleccione lo siguiente:

Accounts -> Terminals -> Assign -> Create

Se mostrata una forma, el siguiente paso es escribir el nombre del dispositivo en /dev. Despues seleccione el tipo de dispositivo, ya sea terminal, impresora o dispositivo removible como un disco duro. Usted deberia despues incluir la ruta completa de cualquier liga al dispositivo.

Administracion de las cuentas de Usuario

GENERACION DE REPORTES DE ACTIVIDAD.

Es posible crear reportes sobre el status de tres aspectos importantes de la operacion del sistema.

1. Passwords:
   reportes sobre cuentas por status de passwords
2. Terminal:
   reportes sobre el status de acceso por terminal
3. Login:
   reportes sobre actividad de usuario, grupo o terminal

Usted puede usar los reportes por proposito de seguridad, por ejemplo, listar los parametros en las base de datos: Protected Password y Terminal Control. Debido a que estos reportes muestran el uso del sistema y de los perifericos, ustd puede hallarlos utiles para afinar y reconfigurar el sistema.
Para todos los reportes, despues de ejecutar la pantalla, se le pide saber si usted quiere dirigir la salida al display, a la impresora o a un archivo.
Usted puede filtrar la salida del display a traves de cualquiera de los programas de paginacion. El programa definido por la variable de ambiente PAGER esta definido como default; si esta variable no esta definida, se usa el programa more. Para la salida a impresora, usted puede dar el nombre del dispositivo de impresion; si no lo da, se usa el destino de impresion default. Para redirigir la salida a un archivo, use el nombre completo de la ruta. No importa que categoria de reporte usted seleccione, siempre se le pedire el dispositivo a donde desea enviar la salida: display, impreso o archivo.

Reportando el status del password.

Para generar reportes basados en el status del password, haga la siguiente seleccion en el sysadmsh:

Accounts -> Report -> Password

El status del password puede ser reportado en varias categorias:

Impeding	reporta sobre las cuentas que estan cerca de expirar
Expired	reporta sobre cuentas de passwords expirados
Dead	reporta sobre cuentas con password muertos
User	reporta sobre un solo usuario
Group	reporta sobre un solo grupo de usuario
Full	lista todas las entradas de la base de datos de password

La opcion Impeding reporta sobre las cuentas que tienen, o pronto tendran passwods vencidos. Esto incluye todas las cuentas con los passwords ya vencidos y los que van a expirar en una semana. A pesar de que una expiracion impeding no es un error, este reporte les permite ver los usuarios que esperan hasta el ultimo momento para cambiar los passwords. Usted puede querer revisar los periodos de expiracion del sistema y de cada usuario basandose en la informacion obtenida aqui.
La opcion Expired reporta todas las cuentas con password vencidos. Estos pueden ser o no ser passwords muertos. Todas estas cuentas necesitan alguna accion administrativa antes de que la cuenta se pueda utilizar; al menos el password debera de ser cambiado.
La opcion User reporta los usuarios individuales que usted especifique, introduzca el nombre del login del usuario para activarla.
La opcion Group reporta sobre la actividad de un solo grupo, este reporte incluye todos los usuarios que pertenecen a un grupo especifico.

Los reportes usan las siguientes abreviaciones:

Dflt
Default
Y, N, D
Yes, No, Default. Algunas selecciones tienen 3 posibles valores: yes, no y el valor default usado por el sistema.

Discos y Cintas

La administracion de medios magneticos, tales como discos y cintas, es importante en cualquier sistema operativo. Los medios magneticos son usados en la gestion de del espacio de disco y en los procedimientos de copia de seguridad (backup) rutinarias que protegen los datos.
Existen varios tipos de sistema de ficheros que se comportan de manera muy diferente, todos ellos pueden aparecer en una misma maquina, pueden incluso compartir el mismo disco, aunque algunos son sistemas de ficheros virtuales que no representan realmente espacio en el disco duro.

Bloques de disco e inodos.

El sistema Unix administra el espacio en disco en unidades llamadas bloques. Los bloques tienen 512 bytes cada uno. Todas las operaciones relacionadas con ficheros trabajan con bloques. Es decir, no se puede crear un fichero o un directorio mas pequeño que un bloque, incluso si solo contiene un byte. Un fichero de 510 bytes utilizara exactamente el mismo espacio en disco que uno de 1 byte.
Ademas los bloques de disco, el sistema de ficheros contiene una lista de nombres de todos los ficheros del disco, asociados a un apuntador al primer bloque de disco correspondiente a cada nombre. Cada nodo y los bloques asociados se almacenan en una entidad llamada “inodo”. Cuando se actualiza un fichero el sistema actualizara el inodo.

Administracion del disco rigido.

Puesto que la actividad principal de sistema Unix esta en el disco rigido interno de la maquina, hay que preocuparse acerca de la gestion de este. El espacio en disco acaba siempre por llenarse con el paso de l tiempo, y existe una tendencia natural a no suprimir material del disco rigido.
La orden “df” proporciona la informacion del espacio ocupado y del espacio libre en todo el sistema de ficheros:

/ (/dev/root): 43996 blocks 132461 i-nodos

df (disk free) tambien informara de la cantidad total de espacio en el sistema de ficheros si se utiliza el parametro -t, por ejemplo:

$ df -t
/ (/dev/root): 43996 blocks 132461 i-nodos
................total: 152558 blocks 19056 i-nodos

La orden "dfspace" (disk free space) realiza el calculo del porcentaje de disco utilizado. Esta orden puede ser utilizada sin argumentos o con una lista con los nombres de los sistemas de ficheros que nos interese conocer el espacio ocupado:

$ dfspace
/ : Disk space: 21.48 MB of 74.49 MB available (28.84%)
Total Disk Space: 21.48 MB of 74.49 MB avaible (28.84%)

La orden "du" (disk usage) informa del numero de bloques de 512 bytes utilizados por cada uno de los subdirectorios:

du /dev
2 /dev/rdsk
2 /dev/dsk
2 /dev/mouse
1 /dev/inet
1 /dev/vems
2 /dev/vdsp
2 /dev/vkbd
1 vmouse
21 /dev

la opcion -s (sumario) produce solamente la aparicion de un total general:

du -s /dev
21 /dev

Por omision, du ignora silenciosamente los ficheros y directorios que no puede abrir. Se utiliza la opcion -r (report) para hacer que du proteste cuando no puede abrir un fichero o directorio.

La orden “ulimit” (user limit) permite restringir el tamaño de un fichero. El valor ulimit es el tamaño de bloques mayor fichero que puede ser creado por un usuario:

```
$ ulimit
4096
$
```

Cuando se intenta crear un fichero mayor que el tamaño permitido por ulimit, el crecimiento del fichero se detendra en ese limite y la orden que esta creando ese fichero fallara enviando un mensaje de error. En el ejemplo anterior, el tamaño maximo del fichero es de 2 MB.
El ulimit implicito es globla del sistema, pero no puede ser modificado para una presentacion de sesion individual. Naturalmente no se puede incrementar el ulimit por alguien diferente al super usuario, pero puede ser reducido:

```
$ ulimit
4096
$ ulimit 1000
$ ulimit
1000
$
```

este cambio permanece durante la sesion actual unicamente.
El administrador del sistema establecera el cambio de ulimit en el /etc/profile del sistema. La configuracion del valor implicito de ulimit se maneja a traves de etc/default/login.

Administracion de discos flexibles.

Antes de utilizar un disco flexible, este debe de contar con un formato, es decir, ser formateado. El formato que se le da a un disco depende de su tipo:

Tipo de Disco	Capacidad
doble cara, doble densidad, 5 ¼’	360 K
doble cara, alta densidad , 5 ¼’	1.2 MB
doble cara, doble densidad, 3 ½	720 K

doble cara, alta densidad, 3 ½	1.44 MB

Tenemos que destacar que el sistema Unix a pesar de manejar el mismo tipo fisico de disco que el sistema operativo MS-DOS, el tipo de formato es distinto, incluso a otros sistemas operativos.
Una vez que el disco ha sido formateado, el sistema Unix proporciona dos maneras de hacer uso de este:

Creando un sistema de ficheros (filesystem)
Accesandolo en bruto (raw acces)
Crear un sistema de ficheros en un disquete, permite utilizarlo como un disco rigido, por ejemplo se pueden crear directorios en el disco, ejecutar cd entre esos directorios, o cp con ficheros. Para esta forma de acceso, se necesita crear una forma de archivos en el disco, y despues montarlos en el sistema de fichero de disco rigido en una posicion especifica llamada punto de montaje.

Los discos utilizados en bruto (raw access), no tendran sistemas de ficheros asociados con ellos y no pueden ser utilizados como un disco rigido. La forma de acceso en bruto a disquete es utilizada generalmente para realizar copias de seguridad de discos.

Otra complicacion se presenta si se desea poder arrancar (boot) la maquina desde un disco flexible, en lugar de hacerlo desde el disco rigido de la maquina. Los discos flexibles con capacidad de arranque son raramente utilizados con los sistemas Unix, pero el primer disco de instalacion del sistema, es un ejemplo de discos con capacidad de arranque.
Los discos con capacidad de arranque deben de contar con un bloque de arranque y un nucleo ejecutable, ya que el sistema operativo entero debe de ejecutarse desde el disquete. Para arrancar con un nuevo disco con capacidad de arranque, generalmente debe de copiarse el primer disco de instalacion del sistema, o a veces los dos primeros discos, y luego editar el contenido de estos.
Los disquetes y tambien los discos rigidos, se gestionan a traves del fichero de dispositivo que designa a este tipo de disco. Estos ficheros especifican:

cual unidad de disco se va a utilizar para la operacion
tipo de formato que el disco tiene
Todos los dispositivos de disco estan incluidos en los directorios dsk (disk) para los tipos de discos con sistemas de archivos (montables) y rdsk (raw disk) para los tipos de disco en bruto. Ambos se encuentran en el directorio /dev.

Los nombres de los ficheros codifican un dispositivo especifico por el tipo de acceso al disco. Por ejemplo, el formato general del nombre de dispositivo para discos flexibles es:

/dev/[r]dsk/f[0,1][5h,5d9,5d8,5d4,5d16,5q,3h,3d][t,u]
donde:

r	indica el acceso en bruto
0,1	selecciona el drive a ser accesado
5h	5.25” alta densidad (1.2 MB)
5d9	5.25” doble densidad 9 sec/track (360 KB)
5d8	5.25” doble densidad 8 sec/track (360 KB)
5d24	5.25” doble densidad 4 sec/track (360 KB)
5d16	5.25” doble densidad 8 sec/track (360 KB)
5q	5.25” cuad densidad (360 KB)
3h	3.5” alta densidad (1.44 MB)
3d	3.5” doble densidad (720 K)

El ultimo parametro, t o u, selecciona la particion que sera accesada, t representa todo el disco, u representa todo el disco excepto el track 0 del cilindro 0. Sin t o u, todo el disco excepto el cilindro 0 seria seleccionado.
Por ejemplo el dispositivo /dev/dsk//f03h se refiere al disco insertado en el drive 0 (unidad A en MS-DOS), de 3.5 pulgadas, con formato de alta densidad (1.44 MB). Aparte de la convencion anterior para el nombre del dispositivo de un disco flexible, se pueden tener alias. A continuacion se muestra un nombre de sispositivo y sus aliases:

dispositivo:	aliases:
/dev/dsk/f0	/dev/dsk/f05d9t
	/dev/dsk/f05d16
	/dev/dsk/f03ht

Se debe de especificar el campo de formato en el nombre del dispositivo cuando se usa la orden format. Sin embargo, cuando se accesa un disco floppy para otras operaciones, como lectura o escritura, el campo de especificacion de formato puede ser omitido.
Los dispositivos de disco rigido siguen la misma organizacion basica, aunque este contrendra en general varias particiones diferentes, o sistemas de ficheros independientes. Cada particion tiene un fichero de dispositivo de bloques (sistema de archivos) y otro en bruto asociado con ella.
Existen varios esquemas de designacion para estas particiones. La usada en el Unix del OPEN DESKTOP es de la forma:

/dev/dsk/n"s"m
donde:
n indica el numero de disco (0 para el primer disco rigido, 1 para el segundo)
m designa un numero de particion (slice)
Para llevar acabo el formato de un disco a mano, se utiliza el comando "format". Esta orden lleva el nombre del camino completo del dispositivo que se desea formatear como argumento por ejemplo:

$ format /dev/rdsk/f03h

El dispositivo en bruto es el utilizado siempre para el formateo de disquetes, ya que el dar formato es una operacion de bajo nivel que requiere acceso al disco basico por debajo del nivel del sistema de ficheros.
La orden /bin/mkfs (make file system) colocara un sistema de ficheros sobre un disquete recien formateado. Es necesario un sistema de ficheros para poder montar un disco.
Cuando se crea un sistema de ficheros, es necesario seleccionar el tipo de sistema de ficheros. Los tipos de ficheros disponibles en Unix del OPEN DESKTOP son:
AFS (Acer Fast Filesystem)
S51K (Unix)
XENIX
DOS
siendo el AFS el tipo de sistemas por omision. El tipo de ficheros se especifica con la opcion -f. Al igual que en format, se debe de especificar el dispositivo en bruto para crear un sistema de ficheros en disco flexible.

$ mkfs -f ufs /dev/rdsk/f03h 2800

Normalmente se utilizara el disco entero, de modo que se puede calcular el numero de bloques a partir del tamaño del disco. Por ejemplo, un disco de 1.44 MB dividido por 512 bytes por bloque da 2880 bloques. Se pueden especificar menos bloques, como en el ejmplo anterior (2800) si se desea, pero asi se desaprovechara el espacio de disco que no se destine al sistema de ficheros.

Montaje de un disco flexible.

Una vez que el disco esta formateado y el sistema de ficheros ha sido creado, se puede llevar acabo el proceso de montar el disco. El montaje de un disco vincula su sistema de ficheros con el sistema de ficheros normal en el disco rigido de la maquina. Cuando se monta un disco flexible (o cualquier otro sistema de ficheros), es posible ejecutar cd en el, hacer copias en el (cp) de ficheros en/y desde sus directorios y utilizar todas las ordenes normales de sistema de ficheros. En muchos sistemas se requiere acceso superusuario para montar un disco flexible.
Normalmente se proporciona un punto de montaje implicito /mnt. Normalmente este directorio esta vacio:

$ ls /mnt
$

Cuando se monta un disco flexible en este punto, el directorio /mnt pasa a tener los contenidos del directorio raiz del disco flexible como se muestra aqui:

mount -f DOS /dev/dsk/f03h /mnt
ls /mnt
datos muestra
#

Observe que se debe de espefificar el tipo de sistema de ficheros con la opcion -f.
Podemos crear un directorio nuevo para usarlo como punto de montaje, o usar uno que ya exista. Si existen ficheros en el punto de montaje antes de montar el disquete, esos ficheros quedaran ocultos por el montaje y no seran visibles hasta que se desmonte el sistema de ficheros montado.

La operacion mount añadira una entrada a la table de montajes del sistema en /etc/mnttab. La tabla de montaje es leida por varios programas del sistema que trabajan con disposistivos montados, tales como df y dfspace.
La desconeccion de la maquina cuando un disquette esta montado, es solo segura si se utiliza la orden shutdown.

La orden mount sin argumentos, informa sobre los dispositivos que estan actualmente montados en la maquina:

mount
/ on /dev/root read/write on Fri Sep 17 19:23:35 1998
/rush1 on /dev/dsk/f03h read only on Sun Sep 19 00:43:16 1998

La orden umount, permite desmontar un disquete o una cinta, para poder retirarllos de la unidad. Su argumento es el nombre del dispositivo, o el nombre del directorio que fue punto de montaje.

umont /dev/dsk/f03h
o bien
umont /mnt

Copia de discos flexibles.

El sistema Unix proporciona varios procedimientos para copiar discos flexibles. En todos los casos hay que formatear el nuevo disco flexible antes de copiarlo. Tambien hay que asegurarse de que el disco al que se este copiando, sea tan grande o mayor que el disco que se esta copiando.
Los tres procedimientos son:

1. Copia manual de un disco montado con cp
2. Copia con dd
3. Copia con cpio

En la copia manual de un disco montado con cp, primero se monta el disco flexible, como se describio anteriormente, en el directorio temporal del disco rigido, y se copian todos los ficheros individualmente a un directorio temporal. Despues se monta un nuevo disquete formateado, con un sistema de ficheros, y se copian los ficheros desde el directorio temporal hasta el nuevo disco. Tambien se puede usar la orden cpio -o que se discutira posteriormente.
La orden dd hace una copia exacta de un disco flexible, sea montable o no. Esta orden se utiliza para copiar medios magneticos exactamente. Por omision, copia su entrada estandar a su salida estandar. Se puede copiar un fichero de la siguiente manera:

$ dd <fich.ent>fich.sal

Para copiar un disco flexible se utiliza dd para copiar el fichero de dispositivo a un archivo temporal. Notese que la orden dd informa del numero de bloques que lee y escribe.

$ dd </dev/rdsk/f03h> /tmp/fich.sal
2880+0 records in
2880+0 records out

luego se reemplaza el disquete con un nuevo disco formateado del mismo tipo y se copia el fichero temporal al disco:

```
$ dd </tmp/fich.sal> /dev/rdsk/f03h
```

Este procedimiento utiliza el nombre de dispositivo en bruto para garantizar una copia completa y exacta del disco flexible entero, y es independiente del tipo de disco flexible y del tipo de sistema de ficheros que este disco contenga.
Al acabar la operacion se suprime el fichero temporal:

```
$ rm /tmp/fich.sal
```

La orden dd, puede ser usada con los argumentos opcionales if=(input file) y of=(output file) de la siguiente forma:

```
$ dd if=/dev/rdsk/f03h of=fich.sal
```

por omision dd hara una copia mediante la lectura y escritura alternadas de bloques de 512 bytes. Se pueden conseguir operaciones mas rapidas utilizando un tamaño de bloque mayor, por ejemplo 5120 bytes. El tamaño del bloque se especifica con la opcion bs=(block size), como se muestra:

```
$ dd bs=5120 </dev/rdsk/f03h>fich.sal
288+0 records in
288+0 records out
$
```

bs=1024 es recomendable para copiar cintas magneticas.
Ademas dd dispone de la opcion conv= para modificar los formatos de datos durante la copia. Se permiten las siguientes conversiones:

ascii	para convertir de EBCDIC a ASCII
ebcdic	para convertir de ASCII a EBCDIC
lcase	para convertir los caracteres a minusculas
ucase	para convertir los caracteres a mayusculas
swab	para intercambiar el orden de bytes de fichero

Finalmente, dd permite omitir los n primeros bloques en la entrada, usando la opcion skip=n; o bien los n primeros bloques en la salida, usando la opcion seek=n.

El procedimiento mount tiene varias ventajas:

Permite aplicar la conveniencia da acceso al sistema de ficheros a discos flexibles y dispositivos de cinta magnetica.
Tambien tiene las siguientes desventajas:

El montaje de un disquete es relativamente lento
El sistema de ficheros estandar ocupa espacio en el disco
No se puede extender un fichero mas alla del espacio disponible en el disco montado
Para resolver estos problemas, el sistema Unix proporciona la orden cpio (copy in/out), que facilita el acceso en bruto a disquetes.
la orden cpio es realmente un programa para almacenamiento que acepta una lista de ficheros y copia estos ficheros en un unico fichero de salida grande, incertando cabeceras entre los ficheros individuales para que puedan ser recuperados.
La orden cpio tiene opciones que permite crear archivos y otras opciones que permiten leer los archivos y volver a cargar los ficheros que hay en ellos. Aqui se llama archivo a un conjunto de ficehros separados por cabeceras (headings).
Los archivos creados con cpio pueden ocupar multiples discos, permitiendo eficientes copias de seguridad en grandes jerarquias de directorios. Ademas cpio preserva la propiedad y los tiempos de modificacion de los ficheros y puede archivar ficheros de texto y binarios.
Puesto que cpio envia su archivo de salida estandar, deberia de utilizarse una orden de esta forma cuando se escriba a un disco flexible:

$ echo nombrefichero | cpio -o > /dev/rdsk/f03ht

La opcion -o (output) le dice a cpio que cree un archivo a partir de una lista de ficheros, como se muestra aqui:

```
$ ls | cpio -o > fich.salida
```

Tambien se puede ejecutar cpio con la lista de nombres de fichero redirigida desde un fichero, en este modo:

```
$ cpio -o > fich.salida < lista.ficheros
```

Otras opciones usadas con la orden cpio y la opcion -o son:

-a (acces)
Reinicializa los tiempos de modificacion asociados con cada fichero
-c (caracter)
Hace que cpio produzca cabeceras internas en formato de caracter en lugar de binario
-H (header)
Permite seleccionar varios formatos, entre ellos crc para chequeos adicionales, y tar para compatibilidad con la orden tar
-B (block)
Para crear bloques de datos en lugar de flujos de datos
-v (verbose)
Le dice a cpio que muestre los nombres de todos los ficheros mientras los lee
-L (link)
Si se desea incluir los vinculos
Frecuentemente cpio va junto con la orden find para generar archivos. La siguiente orden crea un archivo de ficheros con nombres de camino relativos:

```
$ cd
$ find .-print | cpio -oc > /tmp/home.cpio
113 blocks
$
```

Podria escribirse la salida en un fichero de disquete designado el fichero de dispositivo correcto, tal como se muestra aqui:

```
$ find .-print | cpiio -ocvB > /dev/rdsk/f03ht
```

Variando la parte find, puede crearsae un archivo cpio solo con los ficheros que hayan cambiado durante la ultima semana, utilizando la orden siguiente:

```
$ find .-mtime -7 print | cpio -ocv > /tmp/home.cpio
```

La orden -i (input) premite leer los archivos producidos con la opcion -o. El archivo a leer es la entrada estandar del cpio, el cual recrea los ficheros segun los nombres de caminos especificados cuando el archivo fue creado, del modo siguiente:

```
$ cpio -icv < /tmp/home.cpio
```

Si el archivo fue creado con nombres de camino relativos, tales como los ficheros de entrada de “find . -print”, los ficheros se construiran como un arbol de directorios dentro del directorio actual cuando se

ejecuta la orden cpio -i.
Por otra parte, si el archivo fue creado con nombres de camino absolutos (comenzando con /), se utilizaran los mismo caminos absolutos para recrear el fichero.
La utilizacion de nombres de camino absolutos puede ser peligroso, ya que no resulta entonces facil trasladar el arbol de directorios de entrada, la operacion cpio -i puede intentar sobreescribir los ficheros originales.
Algunas de las opciones usadas con la orden cpio y la opcion -i son:

-d (directorio)
Obliga al cpio a crear los directorios necesarios par los ficheros que esta leyendo.
-u (unconditional)
Forzara a sobreescribir a un fichero existente con el mismo nombre que un fichero leido desde el archivo.
-m (modification)
Instruye a cpio para que retenga el tiempo de modificacion de fichero original. Por omision el fichero se crea a la hora actual.
-t (table)
Permite listar solo los nombres de los ficheros y otra informacion. No se crea ningun fichero.
Se puede instruir a cpio para que recarge solo un subconjunto de los ficheros que hay en el archivo proporcionandole un patron en formato de operadores comodines shell en la linea de orden. La orden cpio encontrara todos los ficheros cuyos nombres coincidan con el patron y recargara unicamente estos ficheros. Los patrones deben de ir incluidos entre comillas para impedir que el shell los expanda antes de que cpio los vea.
Por ejemplo:

$ cpio -icvB “*fich” < /dev/rdsk/f03ht

Esta orden recupera todos los ficheros que tengan nombres de caminos acabados en la cadena fich del archivo contenido en el disco flexible de 3.5” de la unidad 0 (A) de 1.44 MB.
Cuando se crea un archivo cpio en el disquete o una cinta, el archivo puede ser mayor que la capacidad del medio magnetico, la orden cpio detecta esta situacion y, cuando el primer disco este lleno, cpio solicitara que sea remplazado, de mosdo siguiente:

$ ls | cpio -ocB > /dev/rdsk/f03ht
Reached end of medium on "output".
To continue, type device/file name where ready.

Con este tipo de peticion de cpio se pueden reemezclar disquetes de diferentes formatos, conmutar entre dos unidades, etc. Sin embargo, generalmente deberia de mantenerse constante el formato del medio correspondiente a un archivo entero.
Si desea detener la orden cpio -i a la mitad, se puede presionar "q" (quit) en la peticion y la operacion terminara, regresando al shell.

Cinta Magnetica.

La version Unix System V Release 4 (SVR4) estandar soporta un cartucho de cinta de cuatro pulgadas en formato QIC y tambien un formato de cinta de alta capacidad DAT basado en SCSI.
Las capacidades de las cintas de formato QIC pueden diferir, las mas comunes para los sistemas SVR4 son 60 MB (QIC 24) y 150 MB (QIC 150). Las unidades de cinta de mayor capacidad pueden ser incapaces de escribir a una capacidad mas baja. Si desea compartir datos, consulte al vendedor para segurarse que la unidad de cinta sea compatible con las otras unidades implicadas.
La siguiente es una tabla de nombres de dispositivo para las diferentes funciones soportadas en las cintas SVR4:

Fichero disp.	Tipo	Comentario
/dev/rmt/c0s0	Continuo	Rebobina tras la operacion E/S
/dev/rmt/c0s0n	Continuo	No rebobina tras la operacion E/S
/dev/rmt/c0s0r	Continuo	Retensiona la cinta antes de E/S Rebobina tras la operacion E/S
/dev/rmt/c0s0nr	Flexible	Retensiona la cinta antes de E/S No rebobina tras la operacion E/S
/dev/rmt/f1q80	Flexible	Rebobina tras la operacion E/S
/dev/rmt/f1q80m	Flexible	No rebobina tras la operacion E/S
/dev/rmt/f1q80r	Flexible	Retensiona la cinta antes de E/S Rebobina tras la operacion E/S
/dev/rmt/f1q80nr	Flexible	Retensiona la cinta antes de E/S No rebobina tras la operacion E/S

Si esta utilizando la cinta estera par aun unico archivo, deseara utilizar el dispositivo con rebobinado para reposicionar la cinta la comienzo despues que se complete la operacion E/S.
Con unidades de cinta continua se puede utilizar cpio para crear y leer archivos en cinta del mismo modo que un disco flexible. Por ejemplo:

$ find .-print | cpio -ocvB > /dev/rmt/c0s0

Para archivos grandes, este puede ser un proceso penosamente lento, pero puede incrementarse el tamaño de bloque que cpio utiliza del modo siguiente:

$ find .-print | cpio -ocv -C 102400 > /dev/rmt/c0s0
La orden tapecntl suele utilizarse para retensionar o reposicionar cintas magneticas. Esta orden no lee ni escribe en cinta; solamente posiciona la cinta para las operaciones normales de lectura y escritura.
Algunas de las opciones usadas con la orden tapecntl son:

-w (wind)
Rebobina la cinta
-r (reinitializa)
Reinicializa la unidad de cinta.
-t (tension)
Retenciona la cinta
-e (erease)
Borra completamente una cinta antigua.
-p (position)
Lleva un numero de fichero como argumento
Observese que si se escribe cualquier fichero en una cinta multifichero excepto el ultimo, todos los ficheros subsiguientes se perderan.

La orden tar es una orden adicional a cpio para archivar en cinta (tape archive).
La orden tar fue diseñada para archivar principalmete en bobinas de cinta de nueve pistas, sin embargo, tar es utilizada frecuentemente para almacenar archivos en disquetes o cintas casete y muchos sistemas antiguos soportan tar en vez de cpio.

Mientras cpio no permite reemplazar un fichero de un archivo con una version mas reciente del fichero, sin recrear completamente el archivo, tar permite añadir nuevos ficheros al final de un archivo existente y reemplazar ficheros al final de un archivo existente y reemplazar ficheros en el archivo. El

reemplazamiento se implementa en tar escribiendo el nuevo fichero al final del archivo. Luego cuando los ficheros son vueltos a cargar, el ultimo fichero reescribira todos los anteriores con el mismo nombre.
El programa tar es un poco mas dificil de utilizar que cpio ya que la gestion del archivo en el medio magnetico la debe de hacer el propio usuario. Es decir, si un usuario crea un archivo con tres versiones de fichero, debe tener cuidado en que la ultima version sea siempre la que desee, ya que tar no puede extraer facilmente ninguna, excepto la ultima ocurrencia de un fichero. Naturalmente, en copias de seguridad la ultima version es generalmente la que se desea, ya que es la version mas reciente.

La orden tar no puede continuar sobre un segundo disco cuando el primero se llena, por lo que sus archivos estan limitados al tamaño maximo del medio de almacenamiento.
La orden tar toma un nombre de fichero, con la opcion -f (file) como argumento principal y este es tratado como el nombre del archivo a crear. Puede ser un fichero normal o un nombre de dispositivo. Los argumentos a continuacion del nombre del archivo son tratados como los nombres de los ficheros a archivar. A diferencia de cpio, tar tomara automaticamente todos los subdirectorios de los directorios designados. Por ejemplo:

```
$ cd /
$ tar -cf /dev/rdsk/f03ht home/steve usr/src
```

Archivara los arboles de directorios home/steve y usr/src, con todos sus subdirectorios, en un disquete de alta densidad.
Si se utiliza - como nombre de archivo, tar utilizara E/S estandar, por lo que la redireccion esta permitida.
Algunas de las opciones usadas con la orden tar son:

-c (create)
Crea un archivo. Destruye el contenido anterior de ese archivo.
-x (extract)
Sirve para recuperar el archivo. Por ejemplo:

```
$ tar -xf /dev/rdsk/f03ht
Tar: blocksize = 20
$
```

para recuperar el archivo en el directorio actual.

-r (replace)
Reemplazar un fichero en un archivo. Por ejemplo:
$ tar -rf /dev/rdsk/f03ht usr/src/steve/bsplit.c
-t (table)
para visualizar una tabla de contenidos de un archivo. por ejemplo:
$ tar -ft /dev/rdsk/f0q15dt
home/steve/datos1
home/steve/datos2
home/steve/cpio.sal
usr/src/bsplit.c
$
-v (verbose)
Produce una lista de los ficheros escritos o leidos desde un archivo.
-w (what)
Hace que tar pida confirmacion al usuario antes de tomar una accion.

Impresoras

Subsistema lp.

Lo orden lp colocara el fichero designado o la entrada estandar, en la cola para una impresora. La orden lp vuelve al shell despues de que el trabajo ha sido puesto en la cola y no cuando la impresion se ha completado. La orden lp puede ser usada de varios modos:

$ cat prueba.txt | lp
o bien
$ lp prueba.txt

La orden lp es especializada en imprimir; si se desea paginar la salida con cabeceras especiales en cada pagina, utilice una herrramienta adicional en la linea de orden, como se ve aqui:

$ pr -h “modelo standar” /etc/lp/model/standard | lp
La orden lp permite varias opciones que pueden modificar el proceso de impresion:

-m (mail)
Proporciona notificacion por el correo electronico, despues de que el fichero ha sido impreso.
-n (number)
Especifica el numero de copias
-t (title)
Controla en contenido de la pagina insigna. Esta pagina identifica la impresion de cada usuario. La opcion -t puede ser usada como sigue:
$ lp “propiedad de $LOGNAME” $HOME/prueba.tx
-o nobanner (option)
Elimina la pagina insigna completamente
-d (destination)
Permite dirigir a una impresora en particular cuando se tiene varias impresoras conectadas a la

maquina, por ejemplo:
$ lp -d ATT470 fich1 fich2 fich3
La orden lpstat proporciona informacion sobre el estado general del sistema lp. Si se ejecuta la orden sin argumento, lpstat lista informacion referente a los trabajo en spool del usuario, como se ve aqui:

$ lp /etc/profile
Request id is ATT470-90 (1 file)
$ lpstat
ATT490-90 steve 1090 Apr 27 19:07

Algunas de las opciones del la orden lpstat son:

-d (default)
Notifica que la impresora es seleccionada por omision (default) al ejecutar la orden lp
-r (running)
Informa si el sistema de impresora esta en operacion o no.
-p (printer)
Determina el estado de una impresora en particular.
Esta opcion puede ser usada con las opciones:
* -l (long)
Visualiza un estado completo de informacion de impresora. Por ejemplo:
$ lpstat -p ATT470 -l

* -D
Produce un resumen corto
-t (total)
Presenta toda la informacion referente al sistema de impresora
La orden cancel permite cancelar un trabajo antes de que haya sido impreso. Su uso es el siguiente:

$ cancel ATT470-86
request “ATT470-86” cancelled

El sistema lp esta controlado por un demonio llamado planificador lp (lp scheduler) que se ejecuta todo el tiempo que el sistema lp esta activo.
Cuando se ejecuta la orden lp para colocar en cola un fichero destinado a la impresora, lp comunica con el planificador lp, informandole que hay un nuevo trabajo listo en la cola.

La orden lpsched, restringida al super usuario, maneja la gestion de cola para impedir que multiples trabajos creados al mismo tiempo compitan entre si por los recursos de la impresora. Tambien gobierna los dispositivos de impresora, detectando cuando cuando una impresora esta inactiva o no funciona.
Puede verse el proceso lpsched listado, con la orden ps -ef. El padre del proceso lpsched es init.
La orden lpsched puede ser utilizada con la opcion:

-r (report)
Determina si lpsched esta ejecutandose en la maquina
La orden lpsched sin argumentos arranca el planificador lp, mientras que la orden lpshut lo detiene.

Impresoras.

Basicamente hay 2 tipos de impresoras: series y paralelas. Estos terminos se refieren al modo en que los datos se transmiten a traves del cable que conecta la computadora a la impresora.
Las impresoras series se conectan generalmente con la computadora a traves de un puerto serie RS-232 o posiblemente a traves de un modem serie.
Las impresoras paralelas se conectan a la computadora a traves de un conector de interfaz paralelo unico, o a veces con un conector DB-25 muy parecido fisicamente a un conector RS-232.
No se puede conectar una impresora paralela a un puerto serie o viceversa, por lo que es importante obtener los cables correctos del fabricante de la impresora o del vendedor del hardware.

Las impresoras PostScript suelen proporcionar solo accceso serie, mientras que las impresoras matriciales y de calidad carta pueden ser series o paralelas. Las impresoras HP LaserJet (y compatibles) pueden incluir ambas interfaces. Cuando se conectan a un puerto serie las impresoras PostScript requieren generalmente un cable modem nulo.
La mayoria de las impresoras incluyen un gran numero de conmutadores para configurar el comportamineto.

Puede utilizar impresoras series y paralelas con el subsistema lp sin dificultad, pero debe de especificar el puerto que la impresora va a utilizar.
Similarmente a las unidades de disco, existen ficheros de dispositivos para ser utilizados como salidas de impresion. A continuacion se muestra una lista de puertos y sus ficheros de dispositivos asociados para sistemas Unix de clase AT:

Nombre PC	Fichero de Dispositivo	Tipo
LPT1	/dev/lp /dev/lp0	Paralela
LPT2	/dev/lp1	Paralela
LPT3	/dev/lp2	Paralela
COM1	/dev/tty00s /dev/term/tty00s	Serie
COM2	/dev/tty01s /dev/term/tty01s	Serie
COM3	/dev/tty02s /dev/term/tty02s	Serie
COM4	/dev/tty03s /dev/term/tty03s	Serie

Muchas maquinas pequeñas estan configuradas con un solo puerto paralelo. Si usted dispone de mas de uno, el fichero de dispositivo /dev/lp1 o /dev/lp2 podria estar presente dependiendo de cuantos puertos paralelos hay disponibles. Con frecuencia es mas facil añadir puertos series adicionales que puertos paralelos, por lo que es probable que se configuren sistemas de multiples impresoras, con impresoras serie, utilizando ficheros de dispositivo /dev/tty02s, /dev/tty03s, etc.

Si desea conectar un tipo de impresora nuevo o inusual, puede necesitar conocer muchas cosas respecto a su comportamiento. El sistema lp opera pasando el fichero a traves de un programa interface que es generalmente un guion shell. Este guion prepara la pagina insigna, configura el puerto de E/S (usado stty) y escribe los datos al fichero de dispositivo correcto. Puede ser necesario modificar esta interfaz para impresoras inusuales.

Son precisos varios pasos para añadir una impresora:

1. Hay que verificar que la impresora este correctamente conectada a la maquina y que este funcionando.
2. Debe de examinarse el guion de interfaz, verificando que hace lo que se espera que haga. En casos raros puede ser necesario modificar un guin para lograr que se ajusten los requerimientos de la impresora.
3. Hay que establecer un conjunto de valores por omision para la impresora de modo que el sistema lp pueda comunicarse con ella, cuando el usuario no especifique opciones especiales en la linea de orden. Tambien puede establecerse un conjunto de filtros para convertir los ficheros a formato de salida de la impresora.
4. Debe informarse al sistema lp que la impresora esta disponible.

5. Finalmente hay que capacitar (enable) la impresora de modo que el sistema lp pueda comenzar a hacer un spool de los trabajos de impresion dirigidos hacia ella.

Para verificar que la impresora este bien conectada y funcionando correctamente, se puede escribir directamente al fichero de dispositivo de modo siguiente:

```
$ cat /etc/lp/model/standard > /dev/lp
```

Si la salida no aparece, o bien el cableado o bien los interruptores de configuracion de la impresora estan prefijados incorrectamente, o bien la propia impresora puede no estar funcionando. Si la salida aparece pero confusa, los interruptores de configuracion estan prefijados incorrectamente.
El test anterior funcionara con la mayoria de las impresoras que aceptan flujos de caracteres normales, tal como las impresoras matriciales. Sin embargo las impresoras que hablan PostScript u otro lenguaje de descripcion de paginas necesitan recibir un programa ejecutable en su lenguaje de control antes de que pueda imprimir algo. Si usted dispone de una impresora PostScript, pruebe este test y vea si se imprime algo:

```
$ cat ficherotest.pd
%!
/Times-Roman findfont 14 scalefont setfont
300 400 moveto
(hola mundo) show
showpage
$ cat ficherotest.ps > /dev/tty00s
```

Si aparece la cadena hola mundo en la impresora, es que esta funcionando. Si este procedimiento cat no funciona con la impresora PostScript, prueba conectandose al puerto de impresora a la velocidad configurada (generalmente 600 baudios) utilizando la orden cu y luego entre al modo interactivo de impresora.

El guion de interfaz es un guion shell que sirve de interfaz entre la orden lp y el fichero de dispositivo que gobierna realmente la impresora. El directorio /usr/lib/lp/model contiene diferentes tipos de estos guiones. Estos guiones son responsables de la definicion de atributos del dispositivo de impresora, tales como:

La velocidad de comunicacion de datos y el control de flujo
Formatear e imprimir el mensaje insigna que separa los diferentes trabajos de salida
Prepara multiples copias a la salida, etc.

La orden /usr/bin/lpadmin, reservada para el superusuario, se usa para especificar valores por omision de las impresoras. Esta orden se utiliza tambien para añadir impresoras, definir el tipo de impresora en el sistema lp y asignar impresoras a clases.
lpadmin puede utilizarse una vez que este seguro que la impresora esta correctamente configurada y que el guon modelo es correcto. Hay que estar seguro que el programa lpsched este corriendo cuando se utiliza lpadmin.
Algunas de las opciones de la orden lpadmin son las siguientes:

-p (printer)	Hace referencia al nombre de la impresora
-m (model)	Especifica el guion modelo de la impresora, por ejemplo standard
-v (device)	Especifica el nombre del fichero de dispositivo asociado a la impresora
-i (interface)	Si se modifica un modelo para un tipo nuevo de impresora, se utiliza esta opcion para especificar el nombre del camino completo de ese guion de interfaz editado
-T (type)	Aqui se especifica el tipo de impresora, que generalmente es el nombre de producto de impresora o un alias para el nombre del producto.
-o (options)	Si no se especifica esta opcion, se utilizaran valores por omision para el trabajo de impresion.
-d (default)	Para especifiacr el valor de la impresora por omision al usar la orden lp
-x (exterminate)	Permite eliminar una impresora del sistema
-c (class)	Especifica la clase de impresora.